

SCSC Seminar Data Safety Evolution



The SCSC held its third Seminar on Data Safety in London on the 14th November 2019. Presentations were given by a number of experts in the field discussing recent developments in the practices and methods in managing the safety risks association with data.

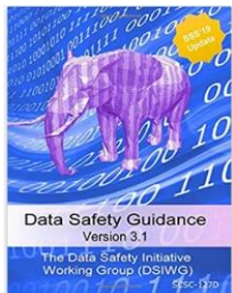
This was a one-day seminar held in the Westminster Park Plaza Hotel in London led by Mike Parsons with individual presentations being hosted by Dave Banham. Approximately 20 delegates attended from a wide range of industries including Aviation, Defence, Healthcare, and Rail. This was the third seminar on this topic, with previous events being held in 2012 ('How to Stop Data Causing Harm' scsc.uk/e209) and 2015 ('How to Stop Data Causing Harm: What you need to know' scsc.uk/e343).

Why Is Data a Safety Problem?

Mike Parsons open the seminar with a recap of why data safety is important and why it needs to be recognised separately from hardware and software considerations.

Mike presented some historical accidents across several sectors where data has been a contributing cause. This included the recent Boeing 737 MAX accidents where data from a faulty angle

of attack sensor led to unintended actuation of the elevator trim that ultimately led to the crashes.



Mike then covered the work of the Data Safety Initiative Working Group (DSIWG) formed in 2013, which has culminated in the publication of a guidance document – Data Safety Guidance (see scsc.uk/scsc-127D and www.amazon.co.uk/gp/product/1793375763). He also covered other DSIWG initiatives currently underway such as the development of an ontology for risk led by David Banham, and the development of tooling to support the implementation of the Data Safety Guidance led by Divya and Martin Atkins (see below).

Introduction to the SCSC Data Safety Guidance

Divya Atkins then presented an introduction to the Data Safety Guidance for those not familiar with its structure and content. Divya described how the document is split into Normative, Informative and Discursive content: Normative covering the formal specification, Informative describing means of compliance and Discursive providing additional information such as list of accidents.

Divya then explained the role of the overarching 4+1 Data Safety Principles that mirror those in software assurance domains and how the sections of the guidance fulfil these principles.

- Principle 1** Data Safety Requirements shall be defined to address the data contribution to system hazards
- Principle 2** The intent of the Data Safety Requirements shall be maintained throughout requirements decomposition
- Principle 3** Data Safety Requirements shall be satisfied
- Principle 4** Hazardous system behaviour arising from the system's use of data shall be identified and mitigated
- Principle 4+1** The confidence established in addressing the Data Safety Assurance Principles shall be commensurate to the contribution of the data to system risk

She then covered the actual process steps, which are structured around ISO31000 - an established risk management standard. In this process, data safety risks are managed by:

- establishing the context
- identifying data safety risks
- analysing and categorising risks by a Data Safety Assurance Level (DSAL)
- evaluating the acceptability of those risk and applying risk control measures.

The first step can be facilitated through the use of an Organisational Data Risk (ODR) Safety Assessment Form. This is a short questionnaire style form that allows an organisation to quickly establish their overall data safety risk exposure by answering 8 questions. The scores for the individual questions are then summed to give an overall ODR value ranging from ODR0 to ODR4 indicating the overall risk exposure from very low to high.

ORGANISATIONAL DATA RISK LEVEL	
Record the total score and use it to determine the ODR level based on the ranges given below. If the first 3 questions' scores sum up to 6 or less then disregard the scores for the remaining questions.	
Score 14 or less	ODR0
Score 15 to 21	ODR1
Score 22 to 37	ODR2
Score 38 to 47	ODR3
Score 48 and above	ODR4
Total Score for this scenario/context:	
ODR Level for this scenario/context:	

DSALs are a new concept created to support the Data Safety Guidance. The guidance uses a traditional risk matrix to categorise data safety risks into DSALs. The DSALs apply to a Data Artefact, which is the item or collections of items of data under concern.

Severity	Likelihood		
	High	Medium	Low
Minor	DSAL1	DSAL0	DSAL0
Moderate	DSAL2	DSAL1	DSAL0
Significant	DSAL3	DSAL2	DSAL1
Major	DSAL4	DSAL3	DSAL2
Catastrophic	DSAL4	DSAL4	DSAL3

Technique	Data Types	DSAL				Notes	Data Property
		1	2	3	4		
Built-in-Test / Built-in-Test Equipment (BIT / BITE)	..D..	-	R	HR	HR	Application tests the data (e.g., at start-up or when requested by an operator).	IC.....V.....
Cyclic / Continuous BIT	..D..	-	-	R	HR	Application applies tests to the data it is processing continuously (e.g., for a live data stream) or periodically (e.g., every nth message, every hour).	IC.Y.....VL.....
Backward recovery	..D..	R	R	HR	HR	If a fault in data has been detected, the system resets to an earlier internal data set, which has been proven consistent.	IC.....
Parity Checks	..D..	R	R	HR	HR	Within data, e.g., Hamming codes, Reed-Solomon, Hagelbarger.	I.....
Automatic Error Correction	..D..	R	R	HR	HR	Detected errors are corrected automatically.	IC.....

A Data Artefact will have a Data Type (Dynamic, Verification, etc.) and the DSAL will relate to the loss of a particular property of that Artefact, such as loss Integrity, Accuracy, Timeliness, Continuity, etc.

The combination of these 3 attributes: Data Type, Property and DSAL are then used to key into several tables of recommended methods and techniques to mitigate those data safety risks.

The process is illustrated through a worked example in the guidance document, relating to a Healthcare case study. The presentation concluded with Divya discussing up-coming areas of work, especially the Data Safety Tooling development, which is supported by a grant from the Lloyds Register Foundation and covered by Martin Atkins later in the seminar.

Data safety - doing it for real

Mark Templeton then presented his own experiences of managing data safety within the military aviation sector. Mark first described his earliest encounters with the data safety problem; he gave an example of SIL4 safety critical systems that communicated over a data-bus, but, at the time, there were no satisfactory established methods or guidance on how to assure the data exchanges between the systems.

He then went on to describe his first experiences of using the Data Safety Guidance to support an airworthiness case for an Unmanned Aerial Vehicle (UAV). He noted that the process was time-consuming and took a lot of hard work, but the discipline of logical examination of data flows, review of mitigations and criticality did lead to a demonstration that

controls were adequate.

Mark said he had then written a Data Safety training course and given this to around 40 people in 4 sessions and this has generated useful feedback. This feedback was used to improve the guidance process definitions and a revalidation of the previous UAV proved to be much easier with this additional clarity. The course feedback and the exercise have now been fed into the latest guidance (v3.1).

Mark then went on to cover another case study – a battle-space scenario with both air and ground actors. In this scenario, almost all of the guidance was applied with about 2 man-weeks of effort. Although some aspects proved useful, such as the data HAZOP guidance, he found that the derived requirements were overwhelming, although this was thought to be a symptom of working at the wrong level.

Mark concluded the presentation with the following observations:

- Techniques within the Guidance are effective
- Data safety HAZOP is particularly good
- The process led to unexpected issues

However:

- The “method” works, but the methods and techniques tables need extending for specific domains
- Manual use of the tables on non-trivial examples can be onerous
- Now needs wider usage and feedback to DSIWG

Applying the SCSC Data Safety Guidance: Practical Considerations

Paul Hampton discussed some practical considerations in applying the guidance in two case studies. The first was to elaborate the Healthcare example that is already in the Data Safety Guidance, and to apply the guidance to derive actual data safety requirements. Paul showed a summary of his working as he followed the guidance to arrive at the final requirement set. Paul noted that, as there were many interconnected systems, Data Artefacts were chosen to align with the individual data-flows leading to in excess of 20 Data Artefacts to assess.



His overall conclusions from the work were:

- Overall the process arrived at a reasonable set of 17 requirements
- The process was only manageable by simplifying the data safety properties under consideration
- Even then, there were many Data Artefacts to consider
- Tooling is essential

In his second case study, he assessed the command and control (C2) link for a commercial Remotely Piloted Aircraft System (RPAS) being used to conduct linear inspections of infrastructure such as electricity pylons.

The analysis was from the perspective of the C2 link provider alone, and so when selecting the Data Artefact, he concluded that there was only one - this being the link itself, as the link provider as no knowledge of the data actually being transmitted across the link.



(Image © Alpha Unmanned Systems)

His overall conclusions from this case study were:

- The process was relatively quick, although there was only one Data Artefact
- Effort spent on copying/pasting from guidance - Tooling is essential
- 60% of recommendations not applicable for this Use Case
- Final derived requirements were a subset of those actually implemented but were not exhaustive - suffers from lack of context
- There is no requirement in the guidance to dictate the level of rigour to be applied in meeting a recommendation

He concluded with some open questions on whether the methods/technique are too data-repository centric and whether more method/techniques for these cases are required.

After the 2 case studies, Paul went on to discuss the role of Organisational Data Risk (ODR) assessments. Although the form was originally intended at the bidding stage, to give a high-level assessment of the data safety risk, it is now seen as being useful in providing more than just raising awareness. Paul then explored its use in helping an organisation tailor its approach to managing data safety risks and how it can complement processes, even in regulated environments such as Aviation. He then concluded with some open questions on whether the ODR should be used to define the level of assurance rigour to apply, and its relationship to existing standards that have assurance levels (SILs/DALs/ASILs etc).

Paul finally looked at the correlation between DSALs and Standards Assurance Levels. In this section he assessed the role of DSALs in Healthcare, where there are standards but no explicit assurance levels, and Aviation where there are standards with Assurance Levels (e.g. DALs). Paul concluded that:

- DSAL severities and likelihoods can be aligned with existing standards
- The DSALs can inform on recommended techniques and methods
- Where a standard has Assurance Levels then DSALs can inform the risk assessment but is independent of the Level
- Overall Data Safety Guidance seems to augment and inform existing standards

Data guidance in defining development of hydrographic data

Dale Callicott presented his view of safety-related data issues that can occur with hydrographic data; this is the data that underpins the maps and navigation systems used by seafaring vessels. He noted that while paper charts could be verified by the Hydrographic Office once produced, this is no longer the case where hydrographic data is being provided to 3rd party suppliers of navigation equipment with electronic map displays.

Dale gave several examples of accidents where hazards such as islands and underwater wrecks were not displayed on the navigation equipment due to issues such as scaling and overlapping icons.

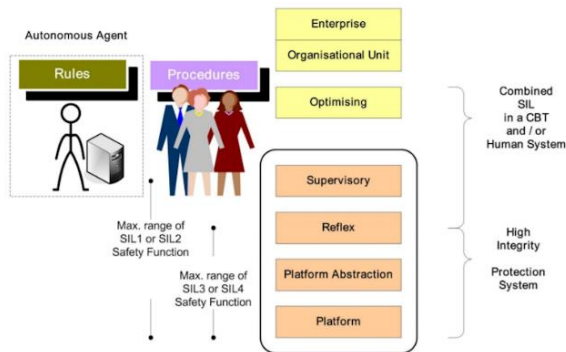
Exploring the Data Safety Model (DSM) as part of the Assurance Solution

Alastair Faulkner discussed the use of a Data Safety Model (DSM) as part of an assurance solution.

Alastair described the architecture of an Information System and then discussed some of the data safety challenges, introducing the concept of strong-data (from sensors) and weak-data (derived from other sources such as data analytics).

Alastair then outlined how the DSM could be applied using a case study involving the autonomous

flight of a drone taking off from an airport and transiting different airspaces.



He described the key steps of the process as the identification of:

- the context, its hierarchy and the actors in the system
- enterprises and organisations and their respective boundaries within the context
- constituent systems (document in the respective system definitions)
- Interface Agreements (including their description and documentation)
- actors, their identities, authentication and authorities
- all information flows within the context and its hierarchy

Throughout, Alastair, highlighted important areas of concern with what he called "Scary Monsters"; these indicated significant and potentially sizable areas of uncertainty where there are no immediately obvious solutions. For example, the methods by which an organisation would investigate a data-safety accident – how can an investigator prove or repudiate a data supply chain stakeholder's contribution to an accident?

The DSM will be covered in more detail in Alastair's forthcoming book, which he is writing in collaboration with Mark Nicholson of the University of York: *"Data-Centric Safety: Challenges, Opportunities and Incident Investigation"*

Data Safety Tooling

Martin Atkins concluded the event by presenting the progress to date in the development of a Data Safety Tool to support the implementation of the Data Safety Guidance. The Tool prototyping phases are funded by a grant from Lloyds Register Foundation. The tool is web based, platform agnostic and supports multiple users.

Martin demonstrated a prototype of the system and ran through real-life examples of how the tool could be used, such as the failed angle of attack sensor in the recent Boeing 737 MAX accident.

He also illustrated the lifecycle and processing context in which the tool would be used.

Report by Paul Hampton, SCSC Newsletter Editor

Project Flight Control System

Leave Project

Manage Data Artefacts

Name	Data Category	Severity	Likelihood	DSAL	Properties
Air Speed	Dynamic	Significant	Medium	DSAL2	I...Y...M.....
Altitude (Pressure)	Dynamic	Minor	High	DSAL1	I..NY...B.....
Altitude (Radar)	Dynamic	Major	Medium	DSAL3	I..CNYO...J..NVL..PQ..B..H..
Angle of Attack	Dynamic	Significant	High	DSAL3	I...A.....
Control Stick	Dynamic	Catastrophic	Medium	DSAL4	I..NYO...R..K..LP..Q.....
Throttle Setting	Dynamic	Catastrophic	Low	DSAL3	
Add new Artefact					



This 1-day seminar will be useful for all those involved in running a complex operation that involves safety. It is aimed at Managers, Operators, Regulators and Assurance staff. If you operate a management or operations centre for your organisation then this seminar is for you.



WWW.SCSC.UK

scsc.uk/e661

THE SAFETY-CRITICAL SYSTEMS CLUB, Seminar:

Management and Oversight of Complex Systems

Thursday 3 December, 2020 - London, UK

This seminar is aimed at those who have to manage, approve, regulate and operate complex systems which have a safety aspect, e.g. Air Traffic Control systems, Nuclear Plant or National Power Transmission systems.

It will cover aspects such as design, operation and manning of control centres, and the use of dashboards and metrics used for monitoring. It will consider the key performance indicators that can be used to measure safety performance.

It will also cover the tools and skills that are required for management and understanding of such systems.

Further details TBC.